UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,960	08/02/2001	Bruno Couillard	35997-215056	4262

26694 7590 01/28/2008
VENABLE LLP
P.O. BOX 34385
WASHINGTON, DC 20043-9998

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
01/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/919,960	**Applicant(s)** COUILLARD, BRUNO	
	Examiner Michael Pyzocha	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10-12,14-27,32 and 33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *10-12,14,21-27 and 33* is/are allowed.

6)☒ Claim(s) *1-8,15-20 and 32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-8, 10-12, 14-27, 32, and 33 are pending.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/03/2007 has been entered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4, 6-8, and 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davies et al. (Security for Computer Networks) in view of Arnold (US 6148400) and further in view of Puhl et al. (US 6223291).

As per claims 1-3, and 15, Davies et al. discloses transferring a first root key between a key provider system and a second other system via an information network comprising the steps of: a) encrypting the first root key using a first super-root key of the key provider system (see pages 160 and 162 where the KKM encrypts the KK and the KKM is therefore the super-root key and the KK is the root key); b) providing within the second other system the second super-root key that is a private key c) transferring the encrypted first root key from the key provider system to the second other system via the information network; d) providing the encrypted first root key to the processor internal to the first secure module of the second other system (see pages 162 and 163); and, e) executing program code on the processor internal to the first secure module to decrypt the encrypted first root key using the second super-root key stored wherein the first root key is useable for at least one of encrypting or decrypting private keys, and wherein a bit length of the first super-root key is greater than a bit length of the first root key, and said bit length of the first root key is greater than a bit length of any of said private keys being encrypted or decrypted (see pages 160-163).

Davies fails to explicitly disclose the use of a secure module in each of the systems with read only memory, the keys only being accessible by the internal processor and the key is other than modifiable and other than accessible outside the module and automatically generating a root key request in dependence on a root key status.

However, Arnold teaches such a secure module (see column 8 line 49 through column 9 line 5) and Puhl et al. teaches such a request (see column 18 lines 23-44).

At the time of the invention it would have been obvious to a person of ordinary skill in the art for each system of Davies et al. to contain a secure module and automatic requests.

Motivation to do so would have been to prevent tampering and eavesdropping (see Arnold column 8 lines 49-67) and to allow root key recovery when a key is compromised (see Puhl et al. column 18 lines 23-25).

As per claims 4 and 16-18, the modified Davies et al., Arnold, and Puhl et al. system discloses the processor internal to the module accesses the second encryption key only in response to a request from a corresponding secure module (see Puhl et al. column 18 lines 23-44 as applied above).

As per claim 6, the modified Davies et al., Arnold, and Puhl et al. system discloses the super-root keys are symmetric (see Davies et al. page 160).

As per claims 7 and 8, the modified Davies et al., Arnold, and Puhl et al. system disclose generating keys within the system (see Arnold column 10 lines 43-64).

5. Claims 5 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al., Arnold, and Puhl et al. system as applied to claim 1 above, and further in view of Menezes et al. (Handbook of Applied Cryptography).

As per claims 5 and 32, the modified Davies et al., Arnold, and Puhl et al. system fails to explicitly disclose that the keys used in the system are public/private key pairs.

However, Menezes et al. teaches the use of public/private key pairs (see pages 25-27).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use public/private key pairs in the modified Davies et al., Arnold, and Puhl et al. system.

Motivation to do so would have been that only the private key must be kept secret (see Menezes et al. page 31).

6. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al., Arnold, and Puhl et al. system (alone or in combination with Spelman, Mason and Ehrsam) as applied to claims 18 and 25, and further in view of Easter et al (US 559889).

As per claim 19 the modified Davies et al., Arnold, and Puhl et al. system fails to disclose the module is FIPS 140 compliant.

However, Easter et al teaches such a compliant module (see column 6 lines 13-21).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to have the module of the modified Davies et al., Arnold, and Puhl et al. system to be FIPS 140 compliant.

Motivation to do so would have been to allow for top security (see Easter et al column 6 lines 13-21).

7. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Davies et al., Arnold, Puhl et al. and Easter et al system as applied to claims 18 and 26, and further in view of Bergum et al (US 5249277).

As per claim 20, the modified Davies et al., Arnold, Puhl et al. and Easter et al system fails to disclose a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

However, Bergum et al teaches such a method of tamper protection (see column 4 lines 7-32).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to apply this method of tamper protection to the modified Davies et al, Arnold, Puhl et al. and Easter et al system.

Motivation to do so would have been to provide maximum key security (see Bergum et al column 4 lines 7-32).

Allowable Subject Matter

8. Claims 10-12, 14, 21-27, and 33 are allowed.

9. The following is a statement of reasons for the indication of allowable subject matter: The prior art teaches updating root keys (see Davies and Spelman), but does not teach the method and system put forth in claims 10 and 21 for updating super-root keys. Specifically the prior art does not teach storing multiple super-root keys in a system nor does it teach any encryption of these super-root keys.

Response to Arguments

Applicant's arguments filed 07/13/2007 have been fully considered but they are not persuasive. Applicant argues that Davies does not teach certain limitations of claims 1 and 15; the combination of Davies with Arnold is improper; Spelman fails to teach certain limitations; the remaining references fail to cure the deficiencies of Davies, Arnold and Spelman.

With respect to Applicant's argument that Davies fails to teach certain limitations of claims 1 and 15 a more detailed description of how the art applies is hereby given with respect to claim 1 which is substantially similar to claim 15:

Davies et al. discloses transferring a first root key between a key provider system and a second other system via an information network comprising the steps of: a) encrypting the first root key using a first super-root key of the key provider system (see page 160 where the KKM encrypts the KK and the KKM is therefore the super-root key and the KK is the root key and page 162 for point-to-point distribution of keys where Banks A and B share a common KKM used for encrypting and transmitting the KK); b) providing within the second other system the second super-root key that is a private key (see page 162 where Bank A and B both share a common key encryption key, KKM, used to exchange KK) c) transferring the encrypted first root key from the key provider system to the second other system via the information network (see page 162 where Bank A acts as the key provider system sending the KSM message); d) providing the encrypted first root key to the processor internal to the first secure module of the second other system; and, e) executing program code on the processor internal to the first secure module to decrypt the encrypted first root key using the second super-root key stored wherein the first root key is useable for at least one of encrypting or decrypting private keys (see pages 162 and 163 where Bank B must decrypt the key using the processor of the TRM describer on pages 144 and 145 in order to use it). Applicant additionally argues the limitation about the length of the keys, but this is no longer a limitation and is therefore moot.

With respect to Applicant's argument that the combination of Davies with Arnold is improper, Applicant specifically argues that the combination would render the system unsatisfactory for its intended use. However, the Arnold reference is merely relied upon for its teaching of the secure module and it would have been obvious to one of ordinary skill in the art to substitute the Secure module of Arnold to store the keys and perform the processing of the memory and processor of Davies to obtain a predictable result of having a module that prevents tampering and eavesdropping. Therefore, the combination would not render the system unsatisfactory so the combination is proper.

Applicant's arguments with respect to claims 4, 5, and 16-18 are moot in view of new grounds of rejection.

Applicant's arguments that Spelman fails to teach certain limitations and the remaining references fail to cure the deficiencies of Davies, Arnold and Spelman are moot as these rejections have been withdrawn and the claims have been allowed over the prior art for the reasons given above.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Mniszewski and Okaue teach methods of using a three key hierarchy for key management.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/27/08